CARRIER STRIKE GROUP TWELVE SPONSORS FLEET/JOINT/COALITION TESTING OF OPEN STANDARDS CHAT TOOL

By Cmdr. Danelle Barrett

Commander, Carrier Strike Group (COMCARSTRKGRU) Twelve initiated and executed a successful combined fleet, joint and coalition test for an open standards chat capability over the NIPRNET Oct. 19, 2005.

Combat Information Systems Officer on USS Enterprise, Lt. Cmdr. Mark Guzzo, and IT2 Laketa Youngwallace and IT1 (SW) Mahogany Moore (right) of Carrier Strike Group Twelve participating in a chat demonstration.

Group Twelve secured the participation and assistance of U.S. Joint Forces Command (USJFCOM), U.S. Pacific Command (USPACOM), Commander, Pacific Fleet (CPF), the Defense Information Systems Agency (DISA), NATO Supreme Allied Command Transformation, U.S. Air Force Command and Control, Intelligence, Surveillance and Reconnaissance Center (AFC2ISRC), Naval Postgraduate School (NPS) and Space and Naval Warfare Systems Command (SPAWAR) to demonstrate tactical chat interoperability using open standards compliant solutions with two of its units underway.

Tactical Chat Challenge in the Fleet

The impetus for the test was the lack of open standards chat tools in the fleet, and the proliferation of stovepipe systems that inhibit interoperability with joint and allied partners. Chat is used in the classified tactical environment by watchstanders and fleet personnel for command and control, and to coordinate logistics, communications and administrative matters. However, it is not used at all on the unclassified side due to known security vulnerabilities with existing chat programs.

Afloat naval units primarily use mIRC (Internet Relay Chat) on Windows workstations, Microsoft Chat on IT-21, and Zircon chat on the Global Command and Control System-Maritime (GCCS-M) as tactical chat tools behind the fleet SIPRNET.

Sametime Meeting Chat is in limited use on the SIPRNET and the Combined Enterprise Regional Information Exchange System (CENTRIXS) among fleet units and coalition partners over separate circuits. Some units also use Multi-Level Secure Chat, government-developed software based on the Dabble protocol (not an open standards protocol). The Defense Collaborative Tool Suite (DCTS) is the approved Department of Defense (DoD) integrated set of off-the-shelf-applications, primarily Microsoft-based, used for collaboration.

While DCTS tools conform to open standards for video and text chat, the clients from different products are not interoperable "out of the box." Additionally, DCTS is not bandwidth friendly, so it is not used by naval units. Some flagships also use InfoWorkSpace (IWS), which requires significant bandwidth and expensive client licenses.

The primary tool used for day-to-day tactical chat operations by the fleet is IRC. However, IRC has inherent security vulnerabilities and limited active commercial development. This hodgepodge of noninteroperable options poses challenges to fleet command and control and shared situational awareness. Therefore, beginning June 2005, COMCARSTRKGRU Twelve, with the significant aid of its aforementioned partners, began planning a fleet, joint and coalition test of open standards Extensible Messaging Presence Protocol (XMPP) tactical chat on the unclassified network.

Government and Industry Support for XMPP

XMPP is an open standards protocol for chat with data in Extensible Markup Language (XML) format. As with any emerging technology or standard, government and industry support is key to proliferation in commercial products, maturation, growth and development of the standard. XMPP has that support. Nov. 30, 2005, the DoD Information Technology (IT) Standards Council (ITSC) unanimously approved the inclusion of XMPP as a mandatory standard in the DoD IT Standards Registry (DISR).

This is significant because it makes XMPP the only approved instant messaging standard approved by the DISR. Government agencies that the DON collaborates with are preparing to use XMPP. For example, the Department of Homeland Security announced in September 2005 that it was moving to XMPP chat.

The Department of the Navy Chief Information Officer (DON CIO) provides the DON voting representative on the ITSC. Additionally, the Internet Engineering Task Force (IETF) formalized core XML streaming protocols as an approved instant messaging and presence technology under the name "XMPP." Major commercial supporters and users of XMPP chat include: Hewlett-

The Department of Defense Information Technology Standards Council (ITSC) unanimously approved the inclusion of XMPP as a mandatory standard in the DoD IT Standards Registry (DISR).

Packard; Jabber, Inc.; Oracle; Sun Microsystems; AT&T Corp.; EDS; Sony; Antepo; Apple; Hitachi; and more. In August 2005, Google announced that its instant messaging capability would be XMPP compliant. There are commercial and open source client and server implementations of XMPP running on Solaris, Windows, Linux, HP-UX, Mac OS X, Palm OS, Windows CE, Symbian OS and any platform capable of running Java Standard (J2EE) or Micro (J2ME) Editions.

Use of an XML-based chat solution will allow the Navy to leverage XML cross domain data guards *(e.g., the USJFCOM XML data guard, part of its Cross Domain Collaborative Information Environment project currently in testing with the National Security Agency)*. This will provide multi-use of a single guard tool for XML relational databases, XML chat and Extensible Hypertext Markup Language (XHTML) data for improved interoperability with other open standards compliant products, which will eliminate the need for the proprietary cross-domain tools currently in place.

Test Objectives, Architecture and Metrics for Success

COMCARSTRKGRU Twelve assembled a test team and coordinated work issues in preparation for testing and approvals to load the chat client software aboard USS Anzio (CG 68) and USS Enterprise (CVN 65). USJFCOM and NPS provided engineering support and equipment ashore to host the test. DISA and SPAWAR assisted in getting the afloat clients through Preferred Product List (PPL) testing.

COMCARSTRKGRU Twelve was adamant about ensuring that all the proper processes and procedures were followed during the testing for loading the client software afloat. These processes included: Shipmain (configuration control), PPL, Interim Authority to Operate, requests for temporary exemption to the Unclassified Trusted Network Protect Policy, etc. Often fleet units load software or install systems without approval because personnel do not know the correct approval processes or the processes may be too cumbersome. This causes configuration management problems for the system commands (SYSCOMs): SPAWAR, Naval Sea Systems Command (NAVSEA) and Naval Air Systems (NAVAIR), which can result in performance or security vulnerabilities on existing shipboard networks and systems.

COMCARSTRKGRU Twelve identified four main test objectives:

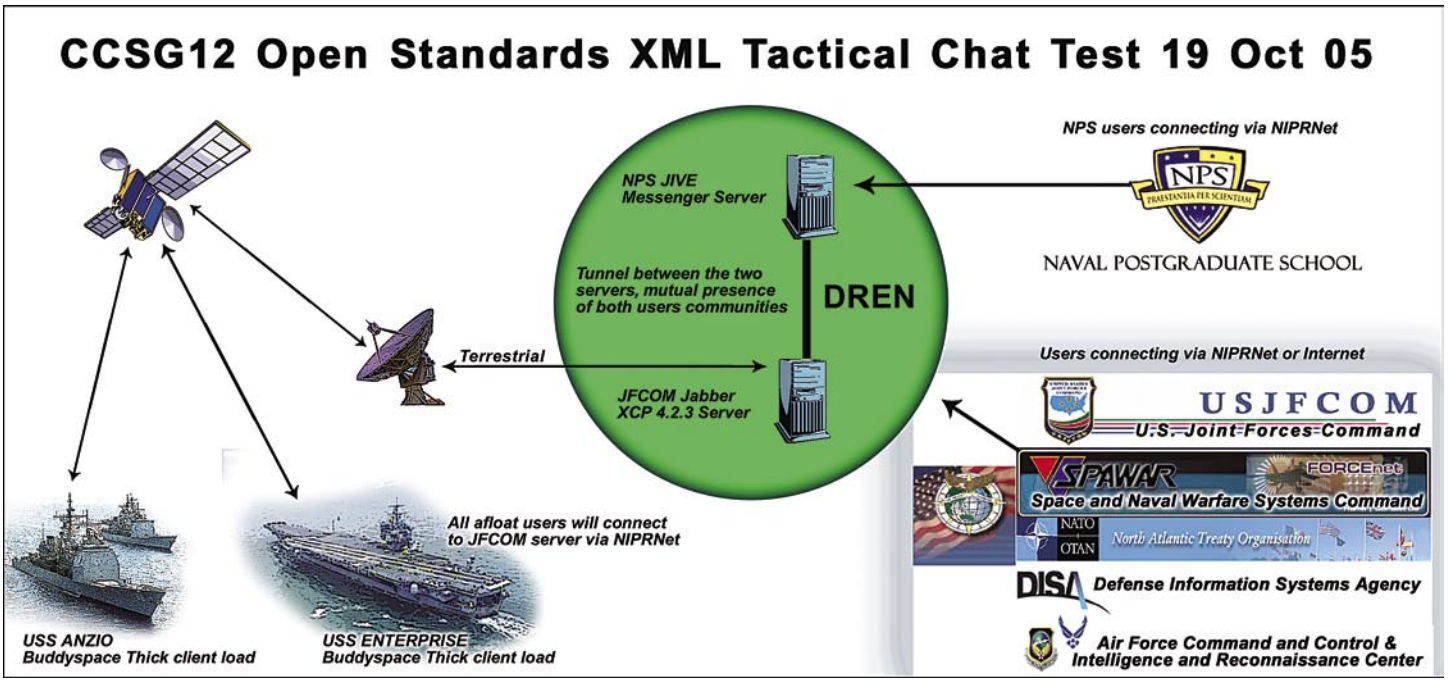
√ Connect and federate the Jabber Jive and Jabber XCP 4.2.5 servers at NPS and USJFCOM respectively, and ensure presence of users and persistence between users on both servers.

√ Load and test different XMPP compliant chat clients at several joint and coalition commands, including units at sea. The mix of clients needed to include thick (client/server) and Web-based clients. Interoperability out of the box among the various clients had to be verified.

√ Hold a chat session with all participants for approximately two hours. Monitor bandwidth for afloat connections and other locations where data could be collected. Analyze bandwidth data to determine functionality of clients in a bandwidth disadvantaged environment, specifically on both large and small ships at sea.

√ Collect subjective data from users about the functionality and performance of the different XMPP client types to determine acceptable and unacceptable user experiences.

Figure 1. Architecture for Carrier Strike Group Twelve chat test.



Metrics for success were established which included:

√ Shipboard bandwidth utilization does not increase significantly (more than five percent).

√ A minimum of two XMPP compliant chat tools successfully interoperate.

√ Chat clients afloat are able to easily connect and function with server ashore.

√ Chat tool is available 100 percent of the time during the test period assuming a stable satellite link.

√ Chat tool is user friendly and intuitive for operators (judged using a survey).

√ Two open standards compliant chat servers are connected with presence of users established.

The test architecture (see Figure 1) included federating two servers together and establishing user presence and persistence for the chat session. USJFCOM was running the Dell PowerEdge 2650 Server and Dual Core 3.0 GHz central processing units (CPU) with four gigabytes of memory. Software included Red Hat Enterprise Linux 3.0 and Jabber XCP 4.2.5.

The NPS server was running on an Intel Mobile Pentium III P3 750 MHz dual processor with one gigabyte of memory. The operating system software was Fedora Core 3 Linux and the XMPP server used Jive Messenger 2.3.0. Both servers operated within the Defense Research and Engineering Network (DREN).

The servers were connected using the XMPP standard server protocol over Transport Control Protocol (TCP) on port 5269. Clients at the Naval Postgraduate School connected to the NPS server. All other clients, including afloat units, connected to the USJFCOM server.

Client software used included:

• USJFCOM: BuddySpace 2.5.1 Pro with USJFCOM enhancements.

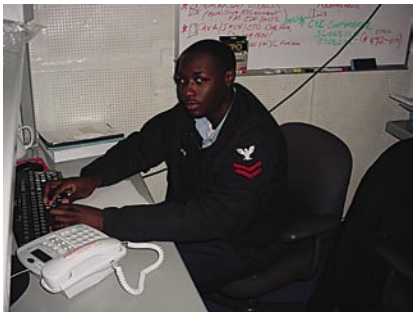
• USPACOM and COMPACFLT: BuddySpace 2.5.1 with USJFCOM enhancements.

• NATO: BuddySpace 2.5.1 Pro with USJFCOM enhancements and Jabber SSL Web Client in nonpolling mode.

• Air Force: Jabber Web Client in polling mode over ports 80 and 443; Jabber Web SSL Client in nonpolling mode over ports 5222 and 5223; and BuddySpace 2.5.1 Pro with USJFCOM enhancements.

• NPS: Exodous thick client 0.9.1 on Windows XP and iChat 3.0.1 on Mac OS 10.4.

• SPAWAR: Jabber Messenger 3.0.2.2 thick client, Jabber SSL Web Client and Jabber Web SSL Client.



IT2 Sherod Cooper of Carrier Strike Group Twelve participating in a combined fleet, joint and coalition test for an open standards chat capability conducted over the NIPRNET Oct. 19, 2005.

• USS Enterprise: BuddySpace 2.5.1 Pro with USJFCOM enhancements.

• USS Anzio: BuddySpace 2.5.1 Pro with USJFCOM enhancements.

Findings

The test conducted Oct. 19, 2005, was totally successful with more than 15 participants from different locations afloat and ashore following a scripted scenario with specific testing criteria. The test results showed that open source chat met the objectives and metrics for success. Four of the users involved in the test were underway on Enterprise and Anzio.

It was important to test the capability on a large ship with more bandwidth and redundant satellite links as well as on a smaller, more bandwidth disadvantaged platform. The test was conducted under normal operations. No special measures were taken to restrict user activity or increase bandwidth on the unclassified network. Because Web clients consume more bandwidth, they are ineffective for use at sea. A thick client solution remains the best alternative for afloat units.

On Enterprise with hundreds of personnel online and only 786 KBps of bandwidth, the BuddySpace thick client performed as good or better than the existing chat program. The same was true on Anzio which had only 128 KBps of bandwidth. In the after testing survey, all afloat users rated it five on a scale of one to five with one being the lowest level of satisfaction. Because the chat entries in BuddySpace were time stamped and persistent, re-entering the chat room posed no loss of situational awareness — an important feature for tactical chat.

Bandwidth utilization is always a concern for afloat units. The results of this test showed that the bandwidth used is supportable by existing satellite links and is comparable or better to existing tactical chat programs. Over the one and a half-hour test period, server bandwidth monitoring captured 10 Mb of client-server data communications for chat and instant messaging. Test participants received up to 600 KBps of TCP message communications from the server.

The most active users sent up to 100 KBps of TCP message communications to the server. The data amount varied with the time users entered and the amount of one-to-one messages. From these estimates, it was determined that passive users averaged 0.11 KBps, while active users averaged 0.13 KBps. Current work by USJFCOM and NPS on compression algorithms for tactical XML chat will only improve bandwidth efficiencies.

The authentication, time stamp and persistent session features in the BuddySpace client were useful from an information assurance perspective. It is not recommended that any chat server afloat be Public Key Infrastructure (PKI) enabled until a mechanism is put in place for non-DoD personnel without certificates to connect.

Recent events such as the tsunami and Hurricane Katrina relief efforts demonstrated the requirements for this type of collaboration via unclassified networks. Because future military collaboration will almost always include coalition partners, other agencies, industry, academia and non-governmental organizations, requiring PKI certifications will most certainly be a limiting factor.

The federation of the servers worked extremely well. Because the Navy will operate any chat architecture in a distributed, federated manner, demonstrating presence of users and their status is an important feature. The Navy must continue to improve synchronization and chat data compression capabilities to ensure efficient use of afloat bandwidth.

In preparation for testing, it was discovered that there is no one place to identify all of the required processes and approvals for loading software afloat. A Rosetta Stone is practically required to identify all the approvals and how to obtain them. As the team worked its way through these processes, more would emerge adding to the bureaucracy for temporary installations for testing initiatives.

For example, a requirement surfaced in September 2005 to add the software to the DON Application Database Management System (DADMS) for Functional Area Manager approval. Fortunately, the requirement was waived so the test could be conducted on time. It was observed that these processes were not easy, nor did they encourage controlled fleet-sponsored innovation and experimentation.

Recommendations

In keeping with consolidated COMCARSTRKGRU Twelve, COMCARSTRKGRU Ten, COMCARSTRKGRU Eight and Commander, Expeditionary Strike Group One messages issued Oct. 17, 2005, which state the fleet operational requirements for open standards solutions for the fleet and implementation of collaborative tools across the naval enterprise architecture, the following recommendations were made by COMCARSTRKGRU Twelve.

• Commander, Naval Network Warfare Command (NETWARCOM) consider a policy making XMPP the approved open standards chat protocol for the fleet and shore Navy, and approve XMPP port use through the fleet firewalls and proxy servers.

• Navy FORCEnet and SYSCOM engineers develop a consolidated plan to implement a distributed, federated, XMPP compliant chat solution for the fleet and eliminate non-XMPP chat programs. Each ship should have its own XMPP chat server so it can continue operations internally during periods when disconnected from the satellite link. Replication and synchronization of chat server data should be carefully engineered.

• Navy FORCEnet and SYSCOM engineers should leverage work done by NPS and USFJCOM to apply compression algorithms to XML chat, which will improve bandwidth efficiencies afloat. Current research and testing achieves XML chat compression by a ratio of 3:1 without noticeably increasing latency of the chat session.

• NETWARCOM work with the SYSCOMs to collectively consider using BuddySpace, the open standard, open source freeware developed by USJFCOM based on the Jabber Instant Messaging model as the software for afloat forces.

• Navy representatives to the DISA Global Information Grid (GIG) Net-Centric Enterprise Services (NCES) Working Group support only XML compliant, bandwidth friendly solutions for the follow-on to DCTS.

• Continue to test XMPP and other open standards compliant collaborative tools in a joint, coalition and interagency environment. The continued development of joint capabilities around open standards should drive Navy solutions particularly when the Navy doesn't have an existing capability.

• Consider XMPP chat and all collaborative tools as enterprise services. Ensure the Navy Marine Corps Intranet (NMCI) adopts XMPP as its instant messaging and text chat solution and that an improved XMPP client be installed on all NMCI workstations. This is particularly important for embarkable staffs moving between the NMCI and afloat network enclaves.

As the Navy continues to put into place key components of the FORCEnet architecture, adherence to open standards collaborative tools, such as those tested during this exercise, will ensure maximum interoperability in future warfighting, peacekeeping and humanitarian relief operations.

Cmdr. Danelle Barrett is assigned to the Standing Joint Force Headquarters, USPACOM. Barrett was the former communications officer on COMCARSTRKGRU Twelve.

The following individuals were part of the XMPP test team and were instrumental in its success: USJFCOM – Ms. Monica Shephard, U.S. Army Maj. Edward McLarney, Boyd Fletcher, Sean Mullin and Brian Raymond. DISA– Diane Boettcher. SPAWAR – Perry Powell, Omar Amezcua, Dennis Magsombol, LorRaine Duffy and Ed Monahan. AFC2ISRC – Charles Martin and Brian Mulkey. NPS – Dr. Don Brutzman, Don McGregor and U.S. Marine Corps Maj. Adrian Armold. NATO – U.S. Navy Cmdr. Eric Kukanich and Mark Lovering. PACOM/CPF – U.S. Marine Corps Col. Kevin Jordan. CPF – Bob Stephenson , Jim Rogers and Rob Thompson. USS Anzio – Lt. j.g. Christopher Miller and Petty Officer Steven Kelley. USS Enterprise – Cmdr. Carrie Hasbrouck, Lt. Cmdr. Mark Guzzo, Ensign Bill Young and Petty Officer Jiacomino Mannino. COMCARSTRKGRU Twelve – IT1 (SW) Mahogany Moore, IT2 (SW) Laketa Youngwallace and IT2 Sherod Cooper. CHIPS